

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)information associated with the Google Accounts
candiceandcompany@gmail.com andchloe.30daysuccessformula@gmail.com that is stored at premises
controlled by Google LLC
(Matter No. 2020R00192)

Case No. 22-907M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Northern District of California
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before 6/3/22 (not to exceed 14 days)

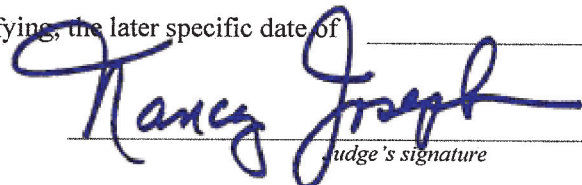
☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Nancy Joseph
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 5/24/22 @ 11:15 A.M.


Judge's signature

City and state: Milwaukee, WIHon. Nancy Joseph, U.S. Magistrate Judge

Printed name and title

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information stored at premises owned, maintained, controlled or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043, that is associated with the following Google accounts:

- Candiceandcompany@gmail.com
- Chloe.30daysuccessformula@gmail.com

ATTACHMENT B

Particular Things to Be Seized

I. Information to be disclosed by Google LLC (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A, for the time period of March 1, 2018 to the present:

a All records and information for the following Google services: Android; Android Market; Apps Marketplace; Apps Script; Blogger; Classroom; Contacts; Dasher Policy; Developer Consoles; Dynamite; Fusion Tables (experimental); GA Plus; Gmail; Google Alerts; Google Apps Administrator Control Panel; Google Bookmarks; Google Calendar; Google Chrome Sync; Google Cloud Print; Google Custom Search; Google Developers Console; Google Docs; Google Drive; Google Groups; Google Hangouts; Google Keep; Google Maps; Google Mobile; Google My Maps; Google Photos; Google Play Music; Google Search Console; Google Sites; Google Sync; Google Takeout; Google Tasks Services; Google Trends; Google Voice; Google+; Jamboard Web and Mobile Apps; Location History; My Devices; Pikeplace; Topaz; Web and App Activity; and YouTube;

b The contents of all text messages, voicemails, recorded calls, emails, and chat messages associated with the account, including stored or preserved copies of chat logs, and emails sent to and from the account, draft communications, the source and destination addresses associated with each communication, the date and time at which each communication was sent,

and the size and length of each communication;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All device information associated with the accounts;

e. All location history associated with the accounts;

f. All search and browsing history associated with the accounts;

g. The types of service utilized;

h. All records or other information stored at any time by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, and files;

i. All records pertaining to communications between the Provider and any person regarding the accounts, including contacts with support services and records of actions taken;

j. All business records and subscriber information, in any form kept, pertaining to the accounts, including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records;

k. All forwarding or fetching accounts relating to the accounts;

l. All data or information about computers and mobile devices registered with or linked to the accounts, including but not limited to, manufacturer name, model number, serial number, media access control address, international mobile equipment identifier number, FCC ID number, and telephone number;

m Subscriber change history; and

n For all Google accounts that are linked to any of the accounts listed in

Attachment A by cookies; recovery, secondary, forwarding; or alternate email address; creation IP address; or telephone number, provide:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses);
3. Local and long distance telephone connection records;
4. Records of session times and durations and IP history log;
5. Length of service (including start date) and types of service utilized;
6. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), MSISDN, International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Station Equipment Identities (“IMEI”));
7. Other subscriber numbers or identities (including temporarily assigned network addresses and registration IP addresses (including carrier grade natting addresses or ports)); and
8. Means and source of payment for such service (including any credit card or bank account number) and billing records.

The Provider is hereby ordered to disclose the above information to the Government within 14 days of the issuance of this warrant.

II. Information to be seized by the Government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 1343 (Wire Fraud) and 18 U.S.C. § 1341 (Mail Fraud) since at least March 2018 to the present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a.** Records and information relating to “30 Day Success Formula”, “Business Solutions LLC”, “Online Biz Development LLC DBA Online Ventures” or any associated corporations, companies, businesses, owners, employees, officers, or affiliates of the above-named companies;
- b.** Evidence indicating how and when the accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the email accounts’ owner;
- c.** Information, regardless of date, that has any tendency to demonstrate the state of mind of the owner and users of the accounts, as well as that of other co-conspirators, with respect to the crimes under investigation;
- d.** Information, regardless of date, relating to the identity or location of any co-conspirators related to the crimes under investigation;
- e.** Any records pertaining to the means and source of payment for services (including credit card or bank account number or digital money transfer account information);
- f.** Information identifying accounts that are linked or associated with the accounts to be searched in Attachment A;
- g.** Any deleted emails documents, information, or communications that were created or deleted in furtherance of the crimes under investigation, or any other communications that Google may retain and any records or information associated with efforts to delete

- those emails or communications—including the dates on, and IP addresses from which any efforts to delete were made;
- h.** The identity of persons who communicated with the email account about matters related to the crimes under investigation, including records that help reveal their whereabouts;
 - i.** Information that constitutes evidence concerning persons who collaborated, conspired, or assisted (knowingly or unknowingly) with the commission of the crimes under investigation;
 - j.** Information related to any digital devices that may have been used to commit the crimes under investigation; and
 - k.** The identity of the person(s) who created or used the account and who communicated with the account about matters relating to the crimes under investigation above, including records that help reveal the whereabouts of such persons.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*information associated with the Google Accounts
candiceandcompany@gmail.com and chloe.30daysuccessformula@gmail.com
that is stored at premises controlled by Google LLC
(Matter No. 2020R00192)

Case No. 22-907M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

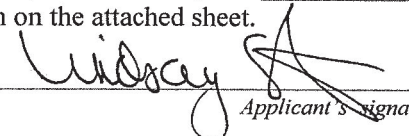
The search is related to a violation of:

Code Section
Title 18, U.S. Code, Sections Mail and Wire Fraud
1341 and 1343

Offense Description

The application is based on these facts:
See attached affidavit.

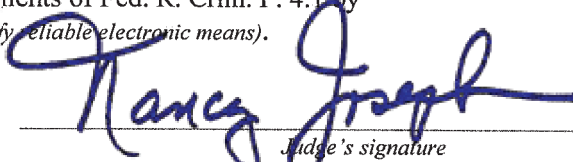
- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days)*: _____ is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

 , FBI
Applicant's signature

Special Agent Lindsay Schloemer, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ *telephone* *(specify reliable electronic means)*.

Date: 5/24/22City and state: Milwaukee, WI


Judge's signature

Hon. Nancy Joseph, U.S. Magistrate Judge
Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Special Agent Lindsay Schloemer, being first duly sworn, state:

INTRODUCTION

1. I make this affidavit in support of a search warrant for information associated with email accounts that are stored at premises controlled by Google LLC (“Google”), an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the Government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. The requested warrant would permit the search and seizure of information associated with the email accounts candiceandcompany@gmail.com and chloe.30daysuccessformula@gmail.com (the “Subject Email Accounts”), which were utilized in connection with the 30 Day Success Formula scheme.

AGENT BACKGROUND

3. I am a Special Agent for the Federal Bureau of Investigation (“FBI”), where I have been employed since November 2014. I am currently assigned to the White Collar Crimes Squad in the Milwaukee Field Office. My current duties include the investigation of financial crimes including investment fraud matters, which are often charged under the wire and mail fraud statutes.

I am also a Certified Public Accountant (“CPA”) and worked as a CPA for seven years prior to my employment with the FBI.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction,” as defined in 18 U.S.C. § 2711. *See* 18 U.S.C. § 2703(d). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated. *See* 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. The FBI is investigating a fraud related to a pyramid scheme advertised to consumers under the name 30 Day Success Formula. I am the lead case agent on the matter. As explained further below, I respectfully submit that there is probable cause to believe that through 30 Day Success Formula, and individuals and entities working on behalf of 30 Day Success Formula, certain individuals conducted a pyramid scheme committing violations of, *inter alia*, 18 U.S.C. § 1343 (wire fraud) and 18 U.S.C. § 1341 (mail fraud), and that the Subject Email Accounts contain evidence of that criminal conduct.

I. Background on Pyramid Schemes and 30 Day Success Formula

7. Pyramid schemes are fraudulent schemes that are advertised to consumers as legitimate business opportunities. A pyramid scheme is where (1) a company’s revenue is derived chiefly from the upfront fees that consumers pay in order to participate in the company’s program

rather than through the sale of an actual product or service, and (2), participants in the program recoup the upfront fees they paid by recruiting additional consumers into the program. Pyramid schemes are inherently fraudulent because their success and growth depend on deceiving consumers about the nature of the program they are paying to join.

8. 30 Day Success Formula was a pyramid scheme that induced individuals to send cash to the perpetrators of the scheme by making false statements, including false promises that individuals who sent funds would receive funds themselves at a later date, when in fact many individuals did not receive such funds. The primary goal of the scheme was to recruit new members to make payments to 30 Day Success Formula on the false promise that these members would themselves receive payments in the future.

II. Overview of the Fraud

30 Day Success Formula

9. The perpetrators of this fraudulent scheme solicited consumers to invest in 30 Day Success Formula by making false promises that consumers would earn large cash commissions after joining 30 Day Success Formula. For example, one set of 30 Day Success Formula marketing materials stated that “when enrolled at Level 4, a mailing twice per month will produce an income of \$81,600 per month.” The investment was misrepresented as low-risk, high-reward, with consumers fraudulently promised a “full, iron-clad, 90-day Money-Back Guarantee.”

10. Potential consumers were directed via online solicitations or solicitations received in the mail to join 30 Day Success Formula by completing an order form and selecting one of several payment options, or “levels” to join at. To join, potential customers were directed to

send only cash in the mail. Several victims interviewed by the FBI indicated 30 Day Success Formula directed the potential customers to place the cash inside a magazine before mailing it.

11. Once a consumer had paid money to enroll in the scheme, the consumer was promised cash in exchange for recruiting new investors. For each new consumer who paid into the scheme, 30 Day Success Formula received a portion of the joining fee (Box #1 on the solicitation letter). A portion of the joining fee also went to the recruiter who referred the individual (Box #2 on the solicitation letter), and to the individual who had recruited the recruiter (Box #3 on the solicitation letter). 30 Day Success Formula marketing materials insisted that an investor could be “totally passive” and still earn significant income.

12. One victim, A.P., noted he sent \$400.00 cash to 30 Day Success Formula, \$400.00 cash to “EZMT Marketing LLC,” and \$200.00 cash to “Alex Zubarev” as instructed by the 30 Day Success’ order form. In return for joining 30 Day Success Formula, A.P. would be sent cash. A.P. sent an additional \$1,200.00 cash to 30 Day Success Formula on the false promise that the company would distribute letters to 1,000 other individuals, and in turn, the victim would receive money from them. 30 Day Success Formula never sent any letters of behalf of A.P., and this victim never received any funds.

13. Other victims who sent funds to 30 Day Success Formula never received the promised returns, or their money back pursuant to the 90 day money back guarantee. One victim interviewed, V.P., mailed a total of \$12,500.00 cash to join 30 Day Success Formula, plus an additional \$1,338.00 for 30 Day Success Formula to send 1,000 letters to potential customers on V.P.’s behalf. V.P. never received any funds, and when V.P. attempted to recoup his original investment pursuant to the 90 day money back “guarantee”, V.P. was unsuccessful.

14. After joining 30 Day Success Formula, the company provided an online product, in the form of online training modules, which were emailed to the consumers. Access to the different online training modules was dependent on the level the consumer joined at. One victim interviewed, K.N., reported she was not able to open the modules, and the information provided was “basic” and could have been found by searching online. Another victim interviewed, R.B., stated that despite the company appearing to sell digital training publications, the whole point of 30 Day Success Formula was to get people to sign up, and then get additional people to sign up below that. Victim A.P. reported never watching the digital marketing trainings he received, and that his sole expectation was that people would mail him money after they received the flyers.

15. As of October 2019, the Better Business Bureau Serving Wisconsin (“BBB”) had received complaints from over 150 consumers regarding 30 Day Success Formula, and estimated that consumers’ total losses exceeded \$150,000. The BBB noted the following consistencies within the complaints filed: the payment to 30 Day Success Formula was requested in cash, the cash was sent to P.O. boxes, 30 Day Success Formula did not refund consumer money despite their money back guarantee, and 30 Day Success Formula did not send out mailers as promised. The complaints came from at least 38 different states and Puerto Rico.

16. As a part of the investigation, the FBI interviewed eight victims, all of whom reported losing money as a result of the scheme totaling approximately \$18,000. Only one of the victims interviewed, R.A., reported receiving a refund of \$89.00 from 30 Day Success Formula in December 2019. Four of the victims interviewed filed a complaint with the FBI via the Internet Crime Complaint Center (IC3.gov).

17. The Wisconsin Department of Agriculture, Trade and Consumer Protection (“WI-DATCP”) opened a civil investigation into 30 Day Success Formula in approximately April

2019. As of January 2020, its investigation uncovered 32 customer complaints, of which, 19 were interviewed by a WI-DATCP investigator. The 32 customer complaints reported losing approximately \$38,000 due to the scheme.

18. Consumer cash payments to 30 Day Success Formula were sent to three different P.O. boxes, all located in the Eastern District of Wisconsin. I have identified Joseph Johnson (“Johnson”) as the lessee of three P.O. boxes associated with 30 Day Success Formula, the first of which was opened in March 2018. I obtained application forms that Johnson submitted to three different United Parcel Service (“UPS”) stores in the Eastern District of Wisconsin to rent three P.O. boxes. The addresses of these three P.O. boxes were listed on different 30 Day Success Formula order forms, with consumers instructed to mail the completed forms and cash deposits to each of the P.O. boxes in order to sign up.

19. Based upon interviews with the owners of the three UPS stores where the boxes were located, I learned the following: that Johnson registered all three P.O. boxes under his name using personal forms of identification, that Johnson was the primary individual who retrieved the mail from these P.O. boxes, that Johnson exclusively used the P.O. boxes to receive mail and never to forward any mail, that Johnson showed up to retrieve mail approximately one to two times each week, and that Johnson stopped coming to one store location to collect the mail in approximately October 2019. The owner from one UPS store location estimated that Johnson’s P.O. box received approximately 150 to 200 pieces of mail addressed to 30 Day Success Formula each day between November 2018 and May 2019.

20. Letters that were collected from the three boxes registered to Johnson were addressed to “30 Day Success Formula” or “Business Solutions LLC.” The aforementioned information led the government to conclude that Johnson was the renter of the P.O. boxes, and that Johnson used the P.O. boxes to collect order forms and money that investors

mailed to 30 Day Success Formula on the false promise of future money. One UPS store owner reported asking Johnson if 30 Day Success Formula was about weight-loss or money; Johnson answered it was about money.

21. Based on the investigation, I determined that 30 Day Success Formula used Internet and email marketing to defraud consumers with false promises of profit for their investments. On or around June 4, 2020, a search warrant issued in the Eastern District of Wisconsin was executed for five (5) email accounts listed on order forms or marketing materials sent to consumers: 30daysuccessformula@gmail.com, fast30daypdf@gmail.com, pdf30day@gmail.com, alfredodelgado7826@gmail.com, and alexandernyc@gmail.com; and one (1) email account for the personal email account of Johnson, GIJoeJr34@gmail.com.

USE OF THE RELEVANT GOOGLE ACCOUNTS

22. On or around February 11, 2022, the government served a Grand Jury subpoena on Google for subscriber information related to the email account candiceandcompany@gmail.com. The records produced from Google identified the subscriber as Candice Cunningham. The last login for the account was on or around January 31, 2022.

23. The FBI conducted a preliminary review of the information contained within the email accounts GIJoeJr34@gmail.com and 30daysuccessformula@gmail.com, and observed the following correspondence with candiceandcompany@gmail.com:

- a. On or around February 9, 2019, GIJoeJr34@gmail.com received an email from United Airlines that identified passengers Joseph E Johnson Jr and Candice Cunningham (“Cunningham”) were ticketed for flight UA524 from Chicago, Illinois to Albuquerque, New Mexico on February 10, 2019. On or around February 11, 2019, GIJoeJr34@gmail.com was forwarded an email from American Airlines from candiceandcompany@gmail.com. The American Airlines email identified passengers Johnson and Cunningham were ticketed on flight AA1359 from Albuquerque, New Mexico to Chicago, Illinois on February 13, 2019.

- b. The government served a Grand Jury subpoena on US Bank, NA (“US Bank”) for bank records associated with account ending in x5249, in the name of Online Biz Development LLC DBA Online Ventures. The records produced from US Bank identified a bank account ending in x5249 was opened on February 11, 2019 in Albuquerque, New Mexico. The signatory on the account was Johnson. Further, Johnson identified US Bank account ending in x5249 as the bank account for 30 Day Success Formula to an investigator at the WI-DATCP.
- c. Based on your affiant’s review of the email communications, it appears that account ending in x5249 was opened at the same time that Cunningham and Johnson were both in Albuquerque, New Mexico.
- d. On or around April 9, 2018 and August 16, 2018, candiceandcompany@gmail.com sent GIJoeJr34@gmail.com an email with an invitation to edit the Google sheet titled “30 Day Success.”
- e. On or around April 11, 2018, GIJoeJr34@gmail.com sent candiceandcompany@gmail.com an email containing an electronic copy of the Mailbox Service Agreement for one of the UPS P.O. boxes leased by Johnson, which was identified in paragraph 18.
- f. On or around June 25, 2018, candiceandcompany@gmail.com sent GIJoeJr34@gmail.com an email containing marketing materials for 30 Day Success Formula. The marketing materials were initially provided to candiceandcompany@gmail.com from “Mughi” with an email address of emailmemuthu@gmail.com. Based on your affiant’s review of US Bank account ending x5249, identified in paragraph 23b, the email address emailmemuthu@gmail.com was paid approximately \$23,348.65 between approximately February 2019 and October 2019 from US Bank account ending in x5249.

- g. On or around February 12, 2019, emailmemuthu@gmail.com sent an email to 30daysuccessformula@gmail.com and Candiceandcompany@gmail.com with an invitation to contribute to the shared folder titled “30 Days Sales Letter Updated Version Printable.”

24. On or around February 14, 2020, the government served a Grand Jury subpoena to Google for subscriber information related to the email account 30daysuccessformula@gmail.com. The records produced from Google identified the subscriber as “Success Formula,” with a recovery email address of chloe.30daysuccessformula@gmail.com. The last login for the account was on or around December 3, 2019. Further, the information provided by Google pursuant to the search warrant executed on or around June 4, 2020, identified chloe.30daysuccessformula@gmail.com was created by the same Internet Protocol (IP) address that created the email account, pdf30day@gmail.com.

25. The FBI conducted a preliminary review of the information contained within the email accounts GJJoeJr34@gmail.com and 30daysuccessformula@gmail.com, and observed the following correspondence with chloe.30daysuccessformula@gmail.com:

- a. On or around May 7, 2019, 30daysuccessformula@gmail.com received an email from an individual who identified himself as a new member of 30 Day Success Formula. The member attached an article from <https://behindmlm.com> titled “30 Day Success Formula bumps gifting fraud payments to \$27,500.” One line in the article stated: “No matter how you cut it though, 30 Day Success Formula is still an illegal cash gifting scheme.” The member wrote in his email to the email address 30daysuccessformula@gmail.com “...Can I get some feed back on this issue? It left me feeling very uneasy and I just received my PDF & Welcome Pkg.” The email was subsequently forwarded to the email address chloe.30daysuccessformula@gmail.com on or around May 10, 2019 with the message “Hello Chloe, I am not sure how to proceed further on this email.”

- b. On or around July 18, 2019, chloe.30daysuccessformula@gmail.com sent GJJoeJr34@gmail.com an email containing marketing materials for 30 Day Success Formula.
- c. On or around July 23, 2019, chloe.30daysuccessformula@gmail.com sent GJJoeJr34@gmail.com an email containing 30 Day Success Formula complaint information reported to the BBB of Wisconsin and Wisconsin Department of Justice.

BACKGROUND CONCERNING EMAIL

26. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail (“email”) access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com. Google also hosts email accounts for domains hosted by other entities. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, Google’s computers are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to confirm the identity of the account user(s) and identify co-conspirators.

27. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number) (Google Profile). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to confirm the identity of the account’s user(s). Based on my training and my experience,

I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

28. In general, an email that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

29. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

30. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

31. A Google subscriber can also subscribe to a range of other services using their

Google account. Google augments its email service by providing a digital calendar (Google Calendar), address book (Google Contacts and Google Groups), online messaging platform (Google Hangouts), to-do list (Google Tasks and Tasks Services), word processor (Google Docs), note-taking service (Google Keep), mobile printing platform (Google Cloud Print), touch-screen accessibility (Google Dasher), social media platform (Google+) and phone number with voicemail and call-forwarding functions (Google Voice). Subscribers may also subscribe to cloud services that allow them to store and share their files (Google Drive), music (Google Play Music), videos (YouTube), photos (Google Photos), teaching materials (Google Classroom), and business ideas (Google Jamboard).

32. Google subscribers can also find directions, save locations, and search geographic areas using Google Maps and create personalized maps using Google My Maps. Subscribers can authorize Google Location Services to record the location history of each device connected to their account. Google subscribers can track their personal or business interests over time using Google Trends. Google Alerts will provide an automatic email alerts every time new content online meets a subscriber's pre-set search criteria. And Google subscribers can gather, visualize, and share large datasets using Google Fusion Tables.

33. In addition, Google provides entrepreneurial services for business subscribers. A Google account may be used to create and sell mobile applications (Android Market; Google Apps Marketplace; Google Developer Consoles; Google Apps Administrator Control Panel) and webpages (Blogger, Google Sites). Subscribers can embed a search engine on their website using Google Custom Search and track the performance of their application or webpage over time (Google Analytics, Google Search Console, Google Plusone).

34. Google will sync its services across multiple devices for an integrated subscriber experience (Google Sync; Google Mobile; Google Chrome Sync). Google tracks the devices authorized to access each subscriber's account (My Devices) and maintain a record of the subscriber's web and application use history across each device. Subscribers may download the

records of their activities across Google services using Google Takeout.

35. In my training and experience, the information available through these additional Google services may constitute evidence of the crimes under investigation because the information can be used to confirm the identity of the account's user(s) and any co-conspirators and indicate whether the account's user possessed illicit information, intended to commit a crime, or was at a particular location at dates and times relevant to the criminal activity.

36. This application seeks a warrant to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The Government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

37. As explained herein, information stored in connection with a Google account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with a Google account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated

with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data such as search history may provide relevant insight into the account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

38. Your affiant knows after consulting with the FBI Cyber Unit that the requested information includes information which Google is able to provide that will assist law enforcement in identifying other accounts associated with the Subject Email Accounts. This information includes any forwarding or fetching accounts¹ relating to Subject Email Accounts, all other Google accounts linked to the Subject Email Accounts because they were accessed from the same computer, all other Google accounts that list the same SMS phone number as the Subject Email Accounts, all other Google accounts that list the same recovery email address as does the Subject Email Accounts, and all other Google accounts that share the same creation IP address as the Subject Email Accounts.

39. Your Affiant knows from training and experience that digital evidence is not limited to computers. Your Affiant has been involved in cases where persons can access the Internet and communicate with other individuals using digital communications devices to include cellular telephones, email devices and personal digital assistants. These devices are frequently found to contain chat communications in the form of short message service (SMS) messages as well as

¹ A forwarding or fetching email account related to the Google Subject Email Accounts would be a separate email account that can be set up to receive copies of all of the email sent to the Google. This information will assist law enforcement in identifying the users of the Subject Email Accounts.

enabling Internet and digital cellular network access.

40. In my training and experience, I have learned that Google keeps records of which gmail.com accounts are accessed from the same electronic device, such as the same computer, through “machine cookies,” which are small pieces of text sent to the user’s device when visiting Google. This warrant requires Google to identify any other accounts accessed by the same device(s) that accessed the Subject Email Accounts described in Attachment A, including accounts linked by machine cookies. The warrant also asks Google to identify any other accounts that are registered with the same email addresses or telephone numbers as the Subject Email Accounts. This warrant will ask that Google provide subscriber information for any accounts thus linked to the Subject Email Accounts.

41. Your Affiant knows from training and experience that the complete contents of email accounts may be important to establishing the actual user who has dominion and control of an email account at a given time. Email accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. Therefore, the content of a given account, including the email accounts that send messages to a given account often provides important evidence regarding the actual user’s dominion and control of an email account.

42. Your Affiant knows from training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as “lol” to express “laugh out loud”), or code words (which require entire strings or series of email conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of an email or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and parentheses “:”) to convey a smile or agreement) to discuss matters. Keyword searches would not account for any of these

possibilities, so actual review of the contents of an email accounts by law enforcement familiar with the identified criminal activity is necessary to find all relevant evidence within the accounts.

CONCLUSION

43. Based on the foregoing, I request that the Court issue the proposed search warrant. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information stored at premises owned, maintained, controlled or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043, that is associated with the following Google accounts:

- Candiceandcompany@gmail.com
- Chloe.30daysuccessformula@gmail.com

ATTACHMENT B

Particular Things to Be Seized

I. Information to be disclosed by Google LLC (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A, for the time period of March 1, 2018 to the present:

a All records and information for the following Google services: Android; Android Market; Apps Marketplace; Apps Script; Blogger; Classroom; Contacts; Dasher Policy; Developer Consoles; Dynamite; Fusion Tables (experimental); GA Plus; Gmail; Google Alerts; Google Apps Administrator Control Panel; Google Bookmarks; Google Calendar; Google Chrome Sync; Google Cloud Print; Google Custom Search; Google Developers Console; Google Docs; Google Drive; Google Groups; Google Hangouts; Google Keep; Google Maps; Google Mobile; Google My Maps; Google Photos; Google Play Music; Google Search Console; Google Sites; Google Sync; Google Takeout; Google Tasks Services; Google Trends; Google Voice; Google+; Jamboard Web and Mobile Apps; Location History; My Devices; Pikeplace; Topaz; Web and App Activity; and YouTube;

b The contents of all text messages, voicemails, recorded calls, emails, and chat messages associated with the account, including stored or preserved copies of chat logs, and emails sent to and from the account, draft communications, the source and destination addresses associated with each communication, the date and time at which each communication was sent,

and the size and length of each communication;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All device information associated with the accounts;

e. All location history associated with the accounts;

f. All search and browsing history associated with the accounts;

g. The types of service utilized;

h. All records or other information stored at any time by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, and files;

i. All records pertaining to communications between the Provider and any person regarding the accounts, including contacts with support services and records of actions taken;

j. All business records and subscriber information, in any form kept, pertaining to the accounts, including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records;

k. All forwarding or fetching accounts relating to the accounts;

l. All data or information about computers and mobile devices registered with or linked to the accounts, including but not limited to, manufacturer name, model number, serial number, media access control address, international mobile equipment identifier number, FCC ID number, and telephone number;

m Subscriber change history; and

n For all Google accounts that are linked to any of the accounts listed in

Attachment A by cookies; recovery, secondary, forwarding; or alternate email address; creation IP address; or telephone number, provide:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses);
3. Local and long distance telephone connection records;
4. Records of session times and durations and IP history log;
5. Length of service (including start date) and types of service utilized;
6. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), MSISDN, International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Station Equipment Identities (“IMEI”));
7. Other subscriber numbers or identities (including temporarily assigned network addresses and registration IP addresses (including carrier grade natting addresses or ports)); and
8. Means and source of payment for such service (including any credit card or bank account number) and billing records.

The Provider is hereby ordered to disclose the above information to the Government within 14 days of the issuance of this warrant.

II. Information to be seized by the Government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 1343 (Wire Fraud) and 18 U.S.C. § 1341 (Mail Fraud) since at least March 2018 to the present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a.** Records and information relating to “30 Day Success Formula”, “Business Solutions LLC”, “Online Biz Development LLC DBA Online Ventures” or any associated corporations, companies, businesses, owners, employees, officers, or affiliates of the above-named companies;
- b.** Evidence indicating how and when the accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the email accounts’ owner;
- c.** Information, regardless of date, that has any tendency to demonstrate the state of mind of the owner and users of the accounts, as well as that of other co-conspirators, with respect to the crimes under investigation;
- d.** Information, regardless of date, relating to the identity or location of any co-conspirators related to the crimes under investigation;
- e.** Any records pertaining to the means and source of payment for services (including credit card or bank account number or digital money transfer account information);
- f.** Information identifying accounts that are linked or associated with the accounts to be searched in Attachment A;
- g.** Any deleted emails documents, information, or communications that were created or deleted in furtherance of the crimes under investigation, or any other communications that Google may retain and any records or information associated with efforts to delete

- those emails or communications—including the dates on, and IP addresses from which any efforts to delete were made;
- h.** The identity of persons who communicated with the email account about matters related to the crimes under investigation, including records that help reveal their whereabouts;
 - i.** Information that constitutes evidence concerning persons who collaborated, conspired, or assisted (knowingly or unknowingly) with the commission of the crimes under investigation;
 - j.** Information related to any digital devices that may have been used to commit the crimes under investigation; and
 - k.** The identity of the person(s) who created or used the account and who communicated with the account about matters relating to the crimes under investigation above, including records that help reveal the whereabouts of such persons.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.